

Don't be that guy/gal...

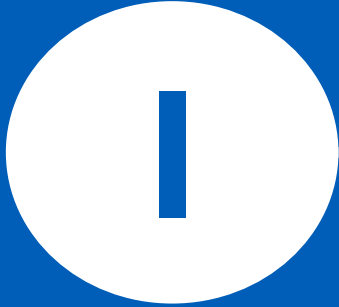
Password Change Sign Up sheet

If you'd like to change your password please fill
out the form below and we will change your
password on the system you indicate.

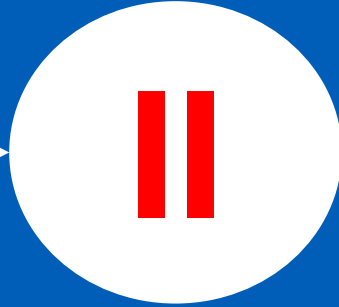
Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scooter49\$	Steele4U2
LIZ JONES	PHONE	89621	4281
Jack H.	Email	Password	Password
Big Ed	Facebook	redsteph	mmmm
Sigm Adams	Pike Pass		beerlover1981

Come See
Me
-Shawn

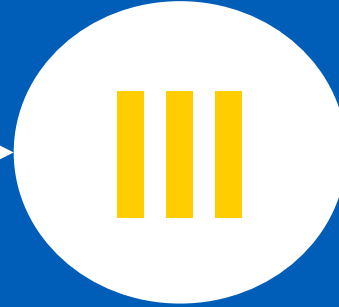
**Conceptual
Foundations
of AIS**



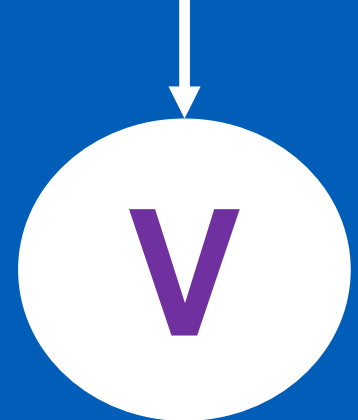
**Transaction
cycles**



AIS control



**AIS investments
and
outsourcing**



**Database
design**





Aalto University
School of Business

AIS Fraud and Control

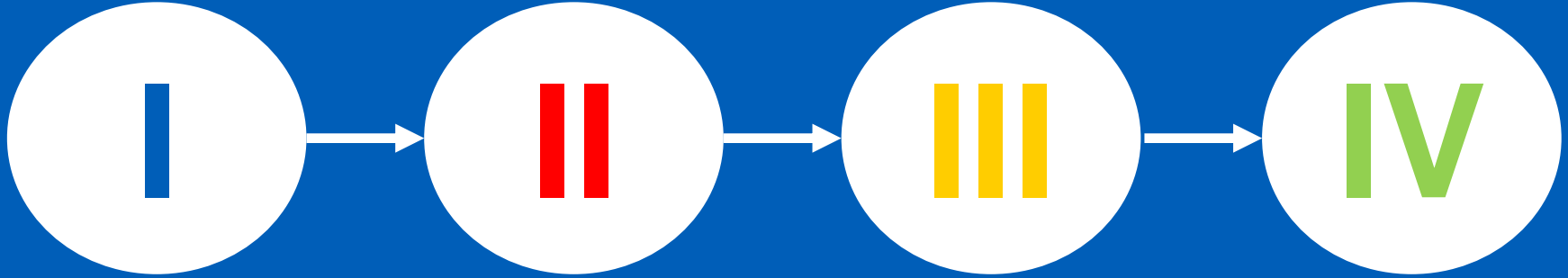
by David Derichs ©
Lecture 3

Why care?

Fraud

Computer
Fraud

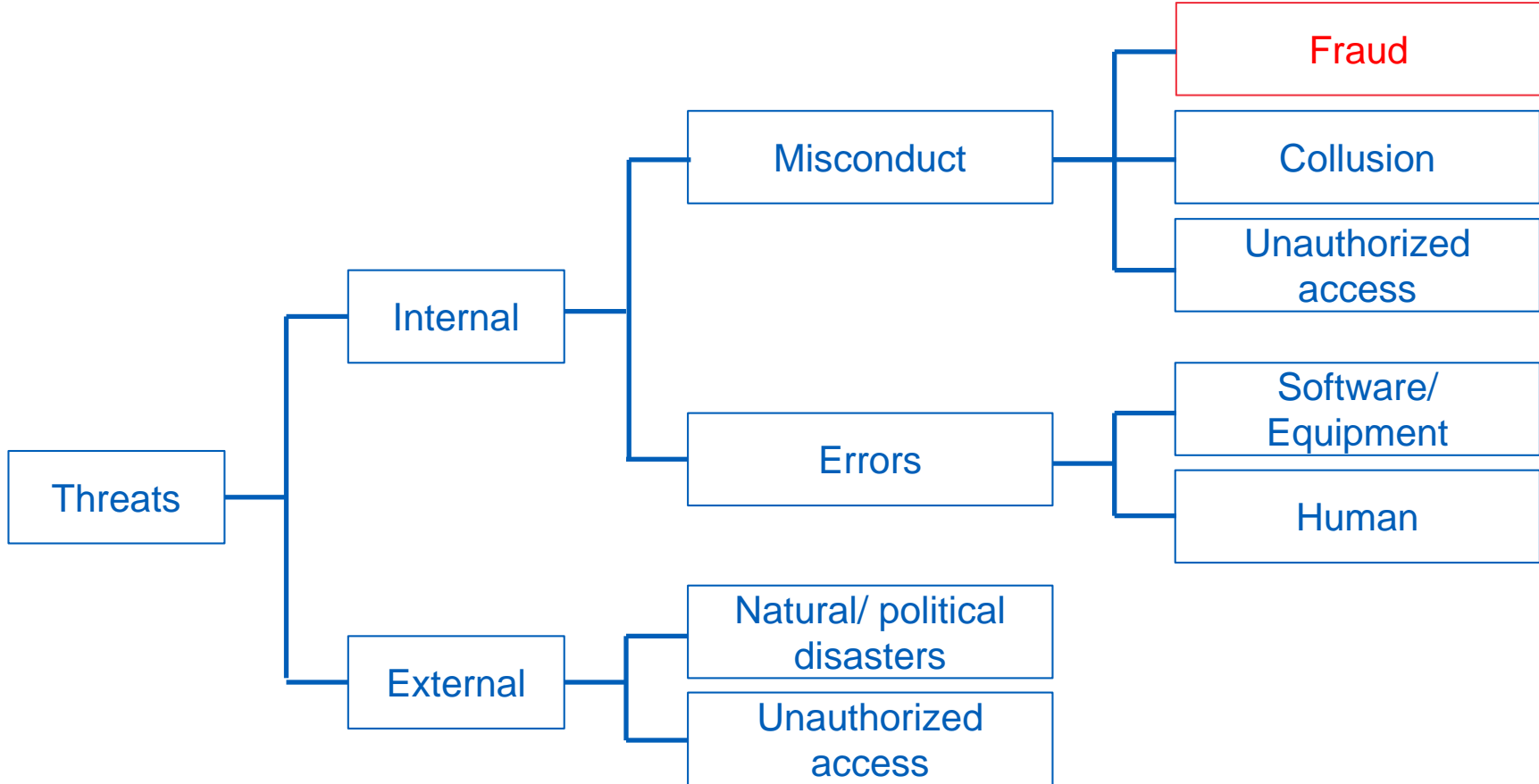
AIS
Control



*Separate
PDF*

Recollection: What internal and external threats do AIS face?

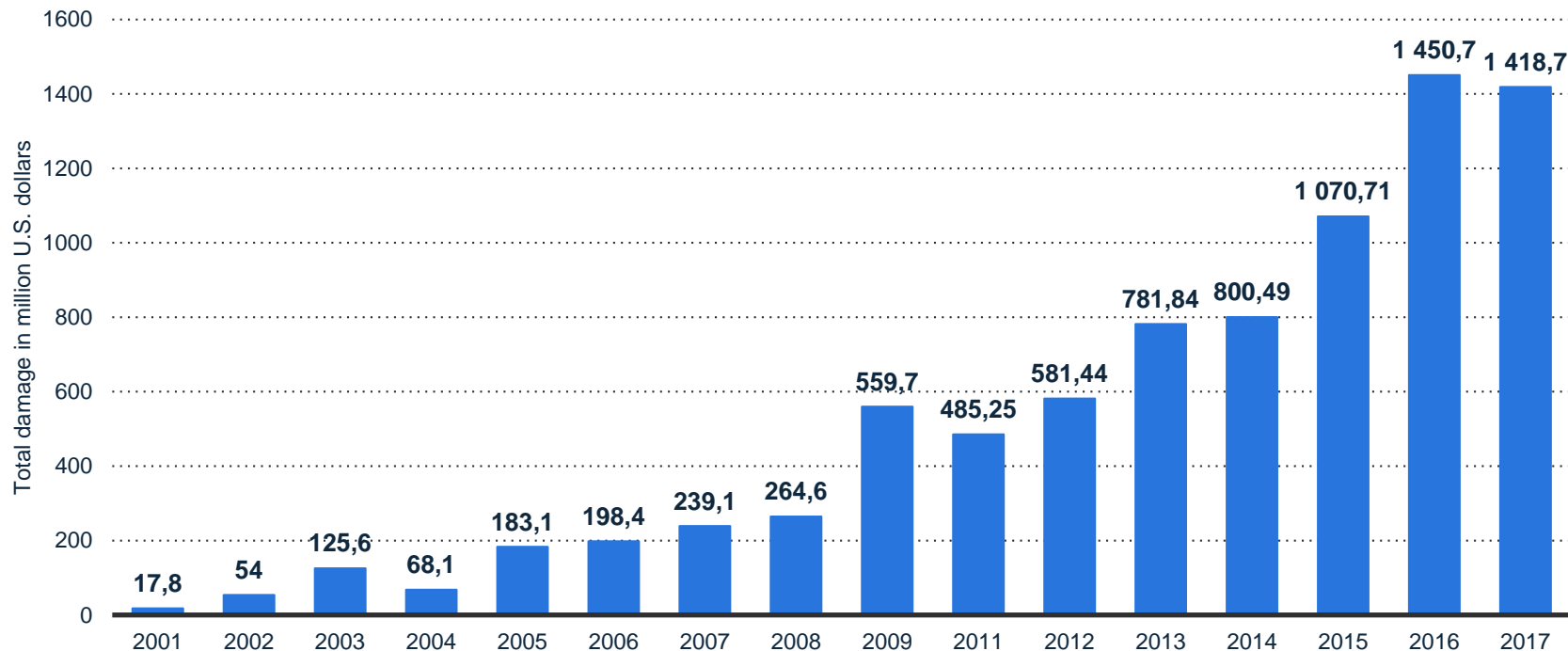
Main internal and external threats



I. Why (should YOU) care?

Cyber crime damage is increasing exponentially!

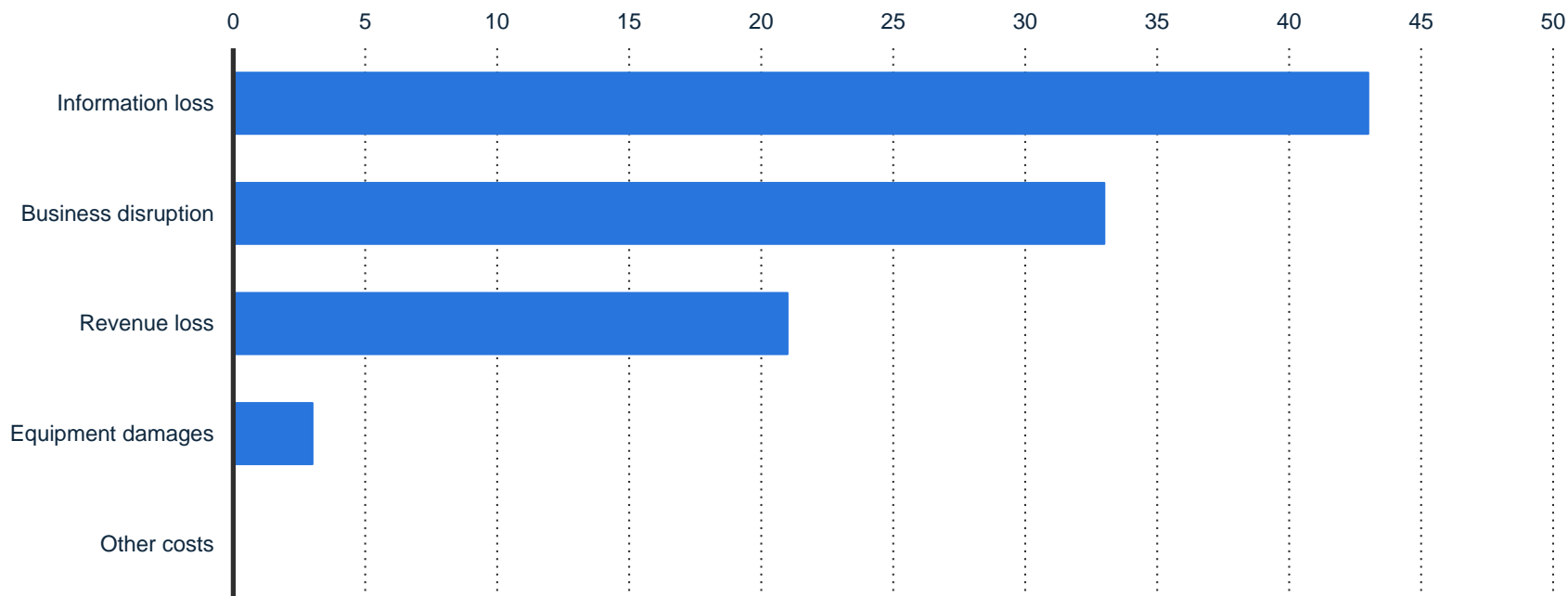
IC3: total damage caused by reported cyber crime 2001-2017 [m USD]



Source: Statista

Highest costs are related to information loss and business disruption

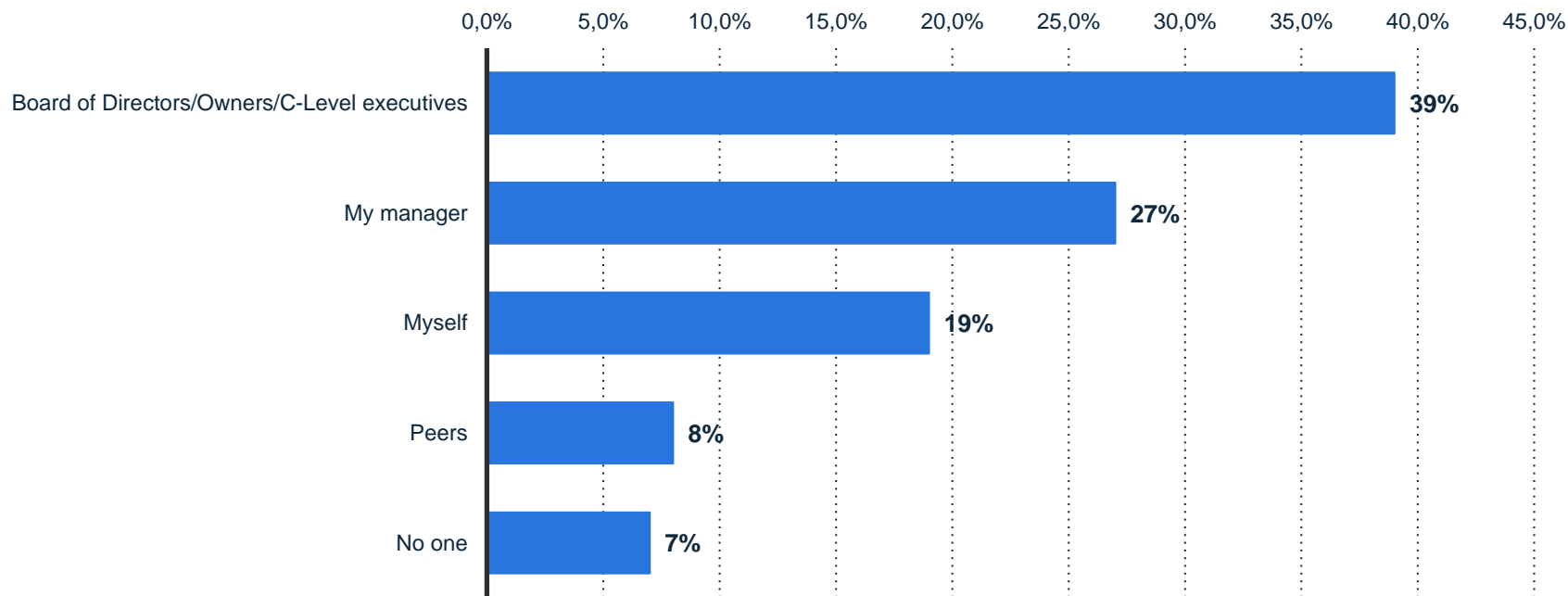
Distribution of annualized costs for external consequences of cyber attacks [%]



Source: Statista

Who exerts the most pressure on you related to IT security?

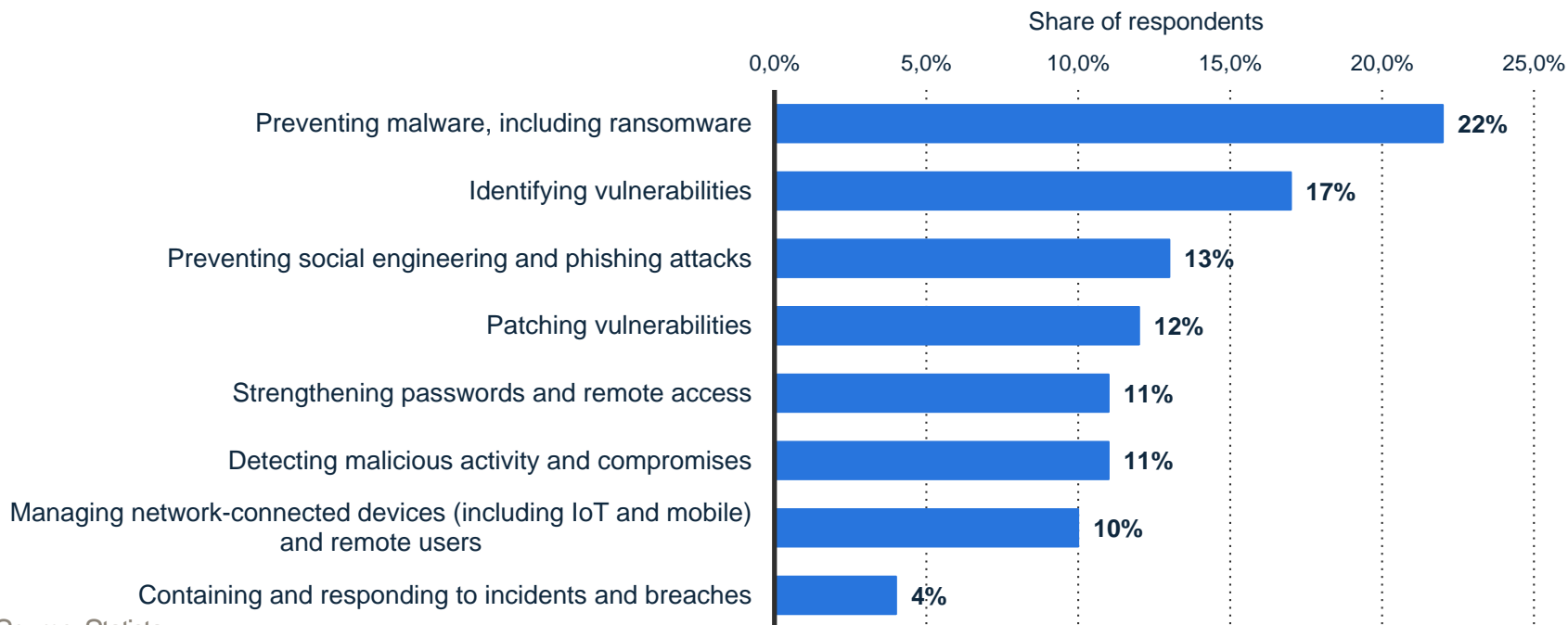
Global human cyber security pressures 2018 [%]



Source: Statista

Which IT security tasks are you facing the most pressure to address?

Most pressing cyber security issues according to IT professionals worldwide 2018




Source: Statista

II. Fraud

Movies: Office space, catch me if you can, the informant

<https://www.youtube.com/watch?v=yLet69-JhW0>

Fraud is commonly referred to as white collar crime

- 
- Any **means** a person uses to gain an **unfair advantage** over another person; includes:
 - A **false statement, representation, or disclosure**
 - A **material fact**, which induces a victim to act
 - An **intent** to deceive
 - Victim **relied** on the misrepresentation
 - **Injury or loss** was suffered by the victim

Fraud comes in four stakeholder categories

Management

Employee

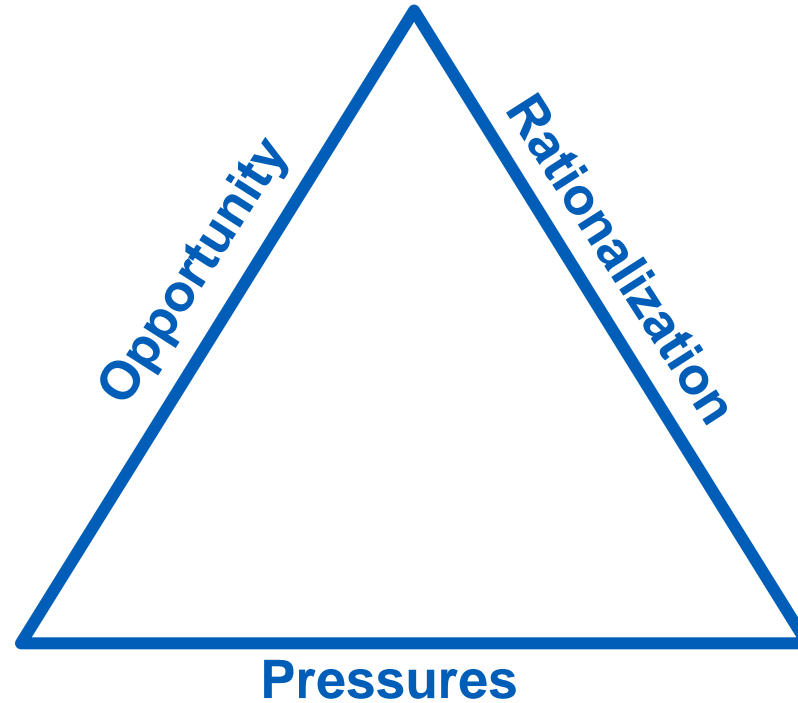
Customer

Vendor

Why do people commit fraud?

Let's think about 'Office Space'!

For fraud to occur there conditions need to be met:



Pressures leading to employee fraud

FINANCIAL

- Living beyond one's means
- High personal debt/expenses
- "Inadequate" salary/income
- Poor credit ratings
- Heavy financial losses
- Bad investments
- Tax avoidance
- Unreasonable quotas/goals

EMOTIONAL

- Excessive greed, ego, pride, ambition
- Performance not recognized
- Job dissatisfaction
- Fear of losing job
- Need for power or control
- Overt, deliberate nonconformity
- Inability to abide by or respect rules
- Challenge of beating the system
- Envy or resentment against others
- Need to win financial one-upmanship competition
- Coercion by bosses/top management

LIFESTYLE

- Gambling habit
- Drug or alcohol addiction
- Sexual relationships
- Family/peer pressure

Pressures leading to financial statement fraud

MANAGEMENT CHARACTERISTICS

Questionable management ethics, management style, and track record
Unduly aggressive earnings forecasts, performance standards, accounting methods, or incentive programs
Significant incentive compensation based on achieving unduly aggressive goals
Management actions or transactions with no clear business justification
Oversensitivity to the effects of alternative accounting treatments on earnings per share
Strained relationship with past auditors
Failure to correct errors on a timely basis, leading to even greater problems
High management/employee turnover
Unusual/odd related-party relationships


INDUSTRY CONDITIONS

Declining industry
Industry or technology changes leading to declining demand or product obsolescence
New regulatory requirements that impair financial stability or profitability
Significant competition or market saturation, with declining margins
Significant tax changes or adjustments


FINANCIAL

Intense pressure to meet or exceed earnings expectations
Significant cash flow problems; unusual difficulty collecting receivables, paying payables
Heavy losses, high or undiversified risk, high dependence on debt, or unduly restrictive debt covenants
Heavy dependence on new or unproven product lines
Severe inventory obsolescence or excessive inventory buildup
Economic conditions (inflation, recession)
Litigation, especially management vs. shareholders
Impending business failure or bankruptcy
Problems with regulatory agencies
High vulnerability to rise in interest rates
Poor or deteriorating financial position
Unusually rapid growth or profitability compared to companies in same industry
Significant estimates involving highly subjective judgments or uncertainties

Opportunity: Condition allowing dishonest acts to be converted into personal gain

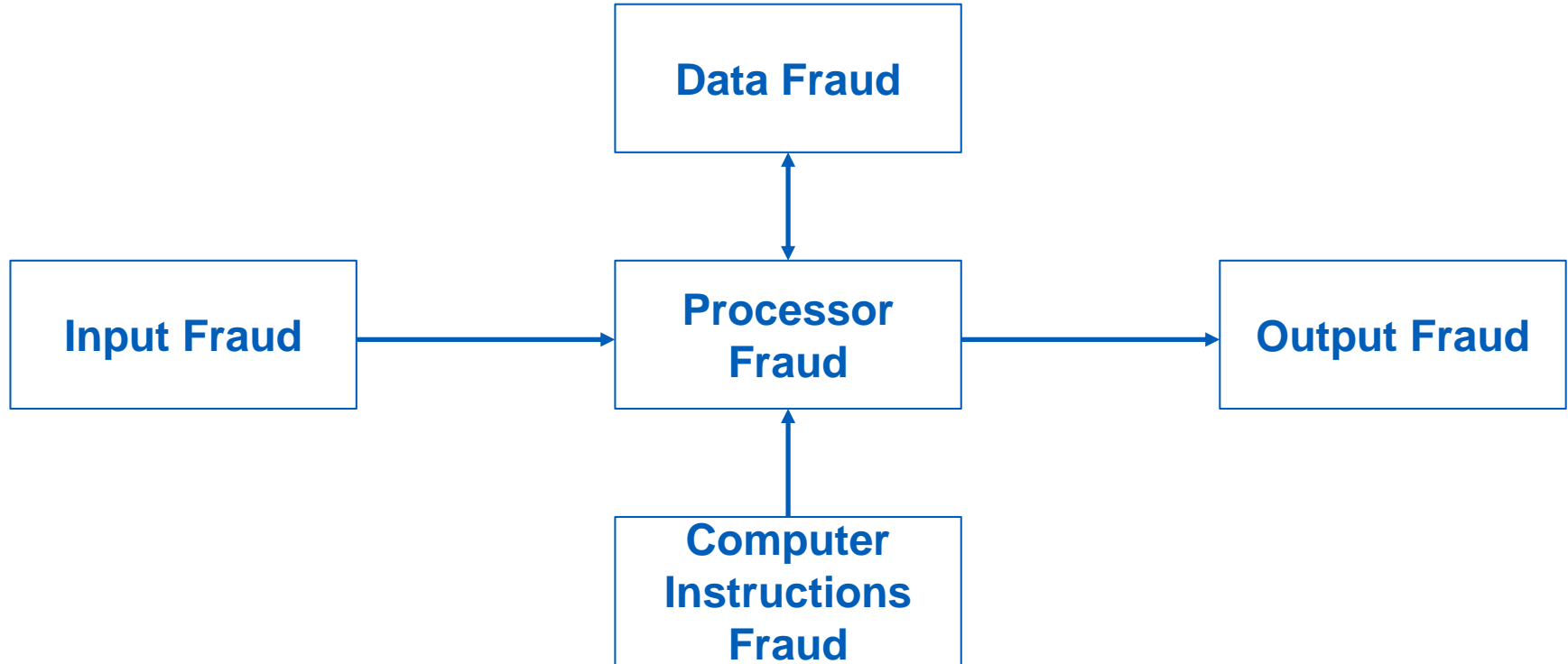
- 
- Opportunity to **commit** fraud (e.g. misappropriation)
 - Opportunity to **conceal** fraud (i.e. accounting equations must be kept in balance):
 - Ponzi scheme
 - Opportunity to **convert** the theft or misrepresentation to personal gain

Rationalization: Excuse to justify fraudulent behavior

- 
- **Justification** – “I only took what they owed me”
 - **Attitude** – “The rules don’t apply to me”
 - **Personal integrity** – “Getting what I want is more important than being honest”


Fraud occurs when people have high pressures, an opportunity to commit, conceal and convert and the ability to rationalize away their personal integrity

Fraud occurs at every step in the data processing cycle



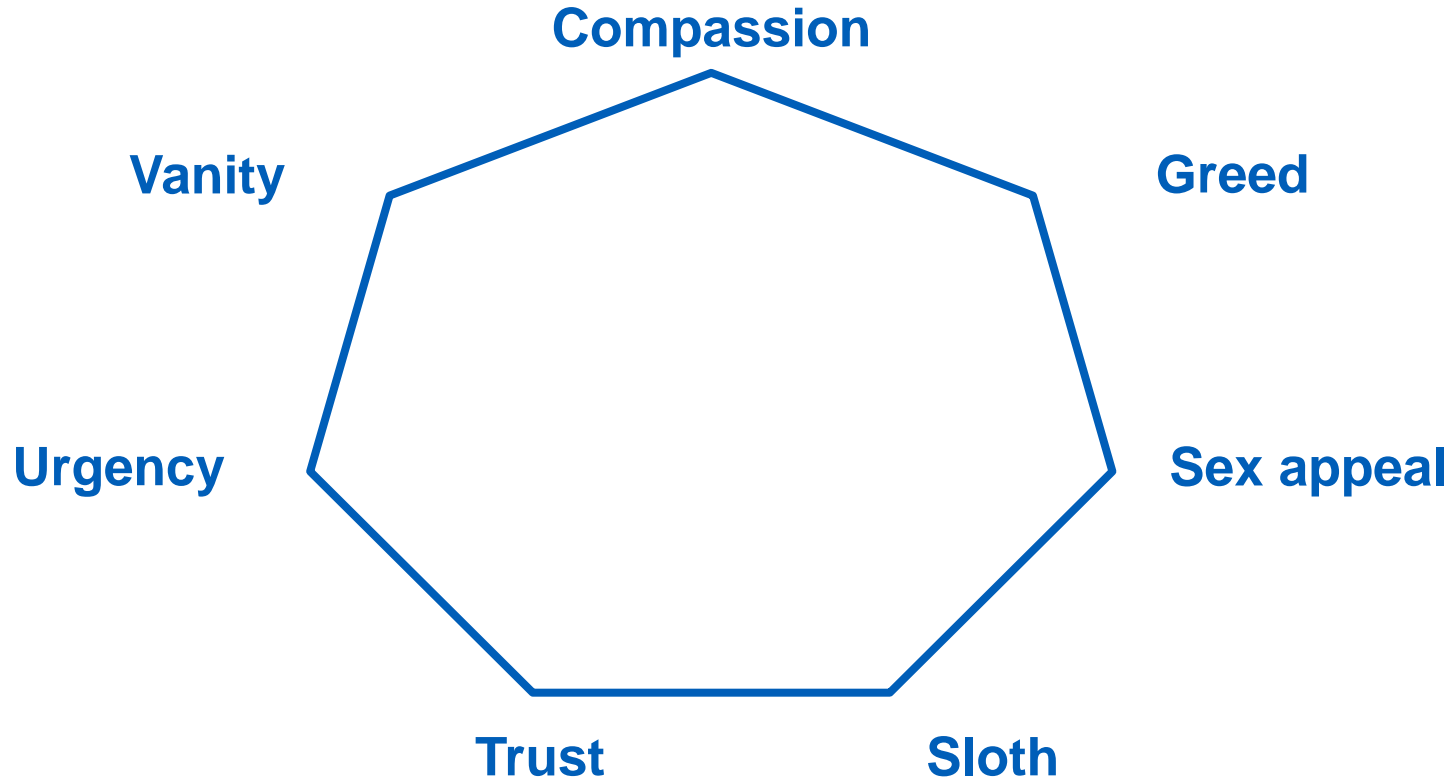
III. Computer fraud

Attacks are commonly divided into three forms


- 
- **Hacking:** Unauthorized access, modification, or use of an electronic device or some element of a computer system
 - **Social Engineering:** Techniques or tricks on people to gain physical or logical access to confidential information
 - **Malware:** Software used to do harm

Why would someone fall victim to manipulation (i.e. social engineering)?

There are seven reasons for falling victim to social engineering



Minimize the Threat of Social Engineering by:

- 
- Never let people **follow you into restricted areas**
 - Never **log in for someone else** on a computer
 - Never **give sensitive information** over the phone or through e-mail
 - Never **share passwords** or user IDs
 - **Be cautious** of someone you don't know who is trying to gain access through you

Hacking – Hijacking and Botnet (1/6)

- **Hijacking**

- *Gaining control of a computer to carry out illicit activities*

- **Botnet (robot network)**

- *Zombies*
- *Bot herders*
- *Denial of Service (DoS) Attack*
- *Spamming*
- *Spoofing*
 - Makes the communication look as if someone else sent it so as to gain confidential information.

Hacking – Spoofing (2/6)

- **Forms of spoofing**

- *E-mail spoofing*
- *Caller ID spoofing*
- *IP address spoofing*
- *Address Resolution (ARP) spoofing*
- *SMS spoofing*
- *Web-page spoofing (phishing)*
- *DNS spoofing*

Hacking – with Computer Code (3/6)

Cross-site scripting (XSS)

- Uses vulnerability of Web application that allows the Web site to get injected with malicious code. When a user visits the Web site, that malicious code is able to collect data from the user.

Buffer overflow attack

- Large amount of data sent to overflow the input memory (buffer) of a program causing it to crash and replaced with attacker's program instructions.

SQL injection (insertion) attack

- Malicious code inserted in place of a query to get to the database information

Hacking – Other (4/6)

- **Man in the middle (MITM)**
 - *Hacker is placed in between a client (user) and a host (server) to read, modify, or steal data.*
- **Masquerading/impersonation**
- **Piggybacking**
- **Password cracking**
- **War dialing and driving**
- **Phreaking**
- **Data diddling**
- **Data leakage**
- **Podslurping**

Hacking – used for embezzlement (5/6)

Salami technique:

- Taking small amounts at a time
 - *Round-down fraud*

Economic espionage

- Theft of information, intellectual property, and trade secrets

Cyber-extortion

- Threats to a person or business online through e-mail or text messages unless money is paid

Hacking – used for fraud (6/6)

- Internet misinformation
- E-mail threats
- Internet auction
- Internet pump and dump
- Click fraud
- Web cramming
- Software piracy

Malware types

- **Spyware**
 - Secretly monitors and collects information
 - Can hijack browser, search requests
 - Adware, Scareware
- **Ransomware**
 - Locks you out of all your programs and data using encryption
- **Keylogger**
 - Software that records user keystrokes
- **Trojan Horse**
 - Malicious computer instructions in an authorized and properly functioning program
- **Trap door**
 - Set of instructions that allow the user to bypass normal system controls
- **Packet sniffer**
 - Captures data as it travels over the Internet
- **Virus**
 - A section of self-replicating code that attaches to a program or file requiring a human to do something so it can replicate itself
- **Worm**
 - Stand alone self replicating program

Thank you!

Questions?